Discussion Paper No. 3

EU Network on the Prevention of Gender-Based and Domestic Violence

Gender-based NCII abuse and cyber hate speech: issues of prevention after the entry into force of the Violence against Women Directive

1.1 Introduction: NCII and cyber hate speech as forms of cyber violence against women and girls

Non-Consensual Intimate Image (NCII) abuse and cyber hate speech are forms of violence in the digital world that disproportionately affect women and girls, especially those at the intersection of different grounds of discrimination. Despite increasing awareness of the effects of NCII abuse and cyber hate speech on mental and physical health and numerous domestic legislative efforts, victims continue to face significant emotional, social, and professional consequences as a result of these behaviours.

In a 2018 report, the **UN Special Rapporteur** on violence against women and girls (VAW) provided a broad definition of online forms of violence:

> The definition of *online violence against women* […] extends to any act of gender-based violence against women that is committed, assisted or aggravated in part or fully by the use of internet and communication technology (ICT), such as mobile phones and smartphones, the Internet, social media platforms or email, *against a woman because she is a woman, or affects women disproportionately*[1].

In the **EU Strategy on victims' rights** 2020-2025, the European Commission defined cybercrime or online crime as 'any type of a criminal offence that is committed online or with a use of computer or online tool,' which 'may include serious crimes against persons such as online sexual offences (including against children), identity theft, online hate crime and crimes against property (such as fraud and counterfeiting).[2] In a **study** for the European Parliament, published in March 2021, the expression 'gender-based cyber violence' has been used, stressing the gendered nature of cyber violence[3]. The study estimates that 4 to 7 % of women in the EU-27 have experienced cyber harassment during the past 12 months, while between 1 and 3 % have experienced cyber stalking. An intersectional dimension has been observed in cyber violence, together with other forms of discrimination and hate speech towards LGBTIQ people, as well as women from racial minority groups and different religious communities.

Gender-based **cyber or ICT-facilitated** violence against women[4] encompasses different forms of violence committed through computer and communication systems, hardware and software. It includes both online and

[1] UNHRC (2018) *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective*, A/HRC/38/47, Para. 23.
[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, EU Strategy on victims' rights (2020-2025), footnote 32, COM/2020/258 final.
[3] European Parliamentary Research Service (2021) *Combating gender-based violence: Cyber violence*, European Added Value Assessment, March 2021, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662621/EPRS_STU(2021)662621_EN.pdf.
[4] Violence in the digital world, ICT-facilitated violence and cyber violence will be used interchangeably.

offline activities involving any ICT devices, whether connected to networks or not.[5] The forms of violence committed in the cyber world that present a gendered dimension can be either specific behaviours that are generally executed online and disproportionately negatively affect women and girls (such as non-consensual dissemination of intimate/private/sexual images), or behaviours that are commonly performed offline (and have been defined in that sense in national legislation) but have presented, especially in recent years, an online dimension (e.g. cyber harassment and cyber stalking). Incitement to hatred and violence, generally referred to as 'hate speech', is a more specific offence, because the behaviour was originally conceived as a form of violence that required certain forms of dissemination (public dissemination or distribution of pictures or other material). In recent years, this behaviour has spread and become exacerbated due to the use of ICT and is increasingly targeted at individuals on the basis of their gender, sexual orientation or gender identity.

Forms of violence in the digital world are numerous; however, it has been shown that with regard to NCII abuse and hate speech, the legislative activism by States has been more decisive in recent years.[6] This demonstrates the gravity of the phenomenon on the one hand, and the willingness of States (and the EU) to take action on the other hand.

1.2 The Istanbul Convention

As it is known, the Istanbul Convention does not expressly refer to cyber violence. However, in General Recommendation No.1, GREVIO, the monitoring body of the Convention, brought within the terms of the Convention behaviours that fall under the definition of digital dimension of violence against women:

> The term "digital dimension of violence against women" is employed to emphasise the fact that this harmful behaviour disproportionately targets women and girls and forms a central element of their experiences of gender-based violence against women. It is violence perpetrated against women and girls that is rooted in the same context of women's inequality and men's sense of entitlement as the psychological, sexual and physical violence experienced by women and girls in the offline world.[7]

In particular, GREVIO considered that sexual harassment, as defined in Article 40 of the Istanbul Convention, is broad enough to encompass the following behaviours: 1) non-consensual image or video sharing; 2) non-consensual taking, producing or procuring of intimate images or videos; 3) exploitation, coercion and threats;4) sexualised bullying: and 5) cyber-flashing. GREVIO provided the following definitions:

> (a) non-consensual sharing of nude or sexual images (photos or videos) of a person or threats thereof include acts of image-based sexual abuse (also known as "revenge pornography")[8];
> (b) non-consensual taking, producing or procuring of intimate images or videos include acts of "upskirting" and taking "creepshots" as well as producing digitally altered imagery in which a person's face or body is superimposed or "stitched into" a pornographic photo or video, known as "fake pornography" (such as "deepfakes", when synthetic images are created using artificial intelligence);
> (c) exploitation, coercion and threats coming within the remit of Article 40 of the Convention include forms of violence such as forced sexting, sexual extortion, rape threats, sexualised/gendered doxing, impersonation and outing;
> (d) sexualised bullying constitutes behaviours such as circulating gossip or rumours about a victim's alleged sexual behaviour, posting sexualised comments under the victim's posts or photos, impersonating a victim and sharing sexual content or sexually harassing others, thus impacting their reputation and/or livelihood, or "outing" someone without their consent with the purpose of scaring, threatening and body shaming; and

[5] S. De Vido, L. Sosa, *Criminalisation of gender-based violence against women in European states, including ICT-facilitated violence*, EELN, 2021, p. 53. https://op.europa.eu/it/publication-detail/-/publication/25712c44-4da1-11ec-91ac-01aa75ed71a1
[6] S. De Vido, L. Sosa, *Criminalisation*, cit.
[7] GREVIO General Recommendation No. 1, para. 24. https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147
[8] Ibid, para. 37.

(e) cyberflashing consists of sending unsolicited sexual images via dating or messaging applications, texts, or using Airdrop or Bluetooth technologies. Some of the above behaviours are commonly known as sexist hate speech.

The Istanbul Convention is complemented by other relevant treaties such as the Convention on Cybercrime of the Council of Europe (Budapest Convention).

1.3 The European Union, in particular the VAW Directive

In a resolution of 2021, the **European Parliament** underlined that 'gender-based cyber violence is a continuation of offline gender-based violence and that no policy alternative will be effective unless it takes that reality into consideration.'[9] It urged the Commission, among others, to use the (at that time forthcoming) directive to criminalise gender-based cyber violence, and to take into consideration the element of intersectionality.

The major recent development in EU law is indeed the Directive on combating violence against women and domestic violence, published in the Official Journal (OJ) on 24 May 2024 (VAW Directive).[10] The **VAW Directive** is based on Article 82(2) and Article 83(1) TFEU. Other developments in EU law are relevant for the analysis, even though they do not have as a primary purpose to prevent and combat violence against women and domestic violence, including, among others, the Digital Services Act,[11] the new Artificial Intelligence Regulation,[12] and the proposal for a revision of the combating child sexual abuse Directive No. 2011/93/EU.[13]

Concerning the VAW Directive, the legal basis of Article 83(1) TFEU has been decisive in establishing minimum rules concerning the definition of criminal offences and sanctions in the area of **computer crime**, which is listed among the Eurocrimes, of a particularly serious nature, showing a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis. As explained in the European Commission's proposal for a Directive:

> The term 'computer crime' in Article 83(1) TFEU covers offences against or intrinsically linked to the use of information and communication technologies. Using such technologies as a means of attack can amplify the severity of the offence in terms of quantity, quality, intensity, target selection and duration, to an extent that cannot be achieved by other means. The minimum rules on crimes amounting to cyber violence against women under this proposal address such offences, which are intrinsically linked to the online environment and the use of such technologies.[14]

The offences related to computer crime, whose elements have been harmonised by the VAW Directive, are the following: non-consensual sharing of intimate or manipulated material (Article 5), cyber stalking (Article 6), cyber harassment (Article 7), cyber incitement to violence or hatred (Article 8). Inciting, aiding and abetting the commission of any of the criminal offences above are punishable as criminal offences (Article 9). The Directive requires Member States to provide effective, proportionate and dissuasive criminal penalties (Article 10).

---

[9] European Parliament Resolution of 14 December 2021 with recommendations to the Commission on combating gender-based violence: cyberviolence (2020/2035(INL)).

[10] Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence, PE/33/2024/REV/1, OJ L, 2024/1385, 24.5.2024 (VAW Directive).

[11] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), PE/30/2022/REV/1, OJ L 277, 27.10.2022, pp. 1–102.

[12] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance), PE/24/2024/REV/1, OJ L, 2024/1689, 12.7.2024.

[13] https://www.europarl.europa.eu/legislative-train/theme-promoting-our-european-way-of-life/file-revision-of-the-combating-child-sexual-abuse-directive

[14] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on combating violence against women and domestic violence, COM/2022/105 final, para. 2.

The November 2024 meeting of the network will focus on Article 5 and Article 8 of the VAW Directive, even though it should be acknowledged that NCII abuse can be used as an instrument to stalk and to harass another person.

1.4 Definitions in the VAW Directive

The VAW Directive provides for the harmonisation of the elements of the crime of **non-consensual sharing of intimate or manipulated material**, which is defined as the intentional conduct of:

a) making accessible to the public, by means of information and communication technologies ('ICT'), images, videos or similar material depicting sexually explicit activities or the intimate parts of a person, without that person's consent, where such conduct is likely to cause serious harm to that person (commonly – though inappropriately – known as revenge porn);
b) producing, manipulating or altering and subsequently making accessible to the public, by means of ICT, images, videos or similar material making it appear as though a person is engaged in sexually explicit activities, without that person's consent, where such conduct is likely to cause serious harm to that person (commonly – though inappropriately – known as deep fake);
c) threatening to engage in the conduct referred to in point (a) or (b) in order to coerce a person to do, acquiesce to or refrain from a certain act.

As has been argued, the concept of **'revenge porn'** is problematic, because 'not all perpetrators are necessarily motivated by revenge, and not all content may be understood popularly as pornographic.'[15] The term 'pornography' does not emphasise the non-consensual nature of the practices, and 'revenge' only focuses on the presumed motive of the perpetrator and excludes the experience and rights of the victims.[16] The concept does not grasp the complexity of behaviours, which vary from the most typical consensual creation of an intimate image during a relationship and the non-consensual distribution of it usually at the end of the relationship, to the consensual (at least at the beginning) sharing of images between friends; from the sharing of intimate images taken from dating sites and apps for non-malicious reasons to the dissemination of images to humiliate, shame or harm a person.[17] The use or dissemination of intimate or private images is gendered. Studies and data have shown that women and girls are the main targets of online digital sexualised violence, and, as a projection of offline violence against women, they are disproportionately affected.[18] Persistent stereotypes and social norms, along with a historically constructed pattern of power relations, tend to blame the woman victim. As has been found, 'while some quantitative studies have found that both men and women have had their images shared without their consent, research has demonstrated that the impact on women whose images have been shared has been much more severe.'[19]

Artificial intelligence (AI) can be exploited to produce **deep fake**, which consists in the creation of convincing images, audio and video hoaxes. The term describes 'both the technology and the resulting bogus content, and is a portmanteau of deep learning and fake.'[20] Deep fakes might "invent" art works or produce music, but they might be also used for political misinformation, fraud and ruining a person's reputation. Non-consensual deep

[15] T. Kirchengast, T. Crofts, 'The Legal and Policy Contexts of "Revenge Porn" Criminalisation: The Need for Multiple Approaches', in *Oxford University Commonwealth Law Journal* 19 (1), 2019, p. 4.
[16] C. McGlynn, E. Rackley, R. Houghton, 'Beyond "Revenge Porn": The Continuum of Image-based Sexual Abuse', in *Feminist Legal Studies,* 25, 2017, p. 25.
[17] Ibid. See also S. De Vido, L. Sosa, *Criminalisation,* cit.
[18] N. Henry and others, *Image-Based Sexual Abuse: A Study on the Causes and Consequences of Non-Consensual Nude or Sexual Imagery*, New York, Routledge, 2020.
[19] S. Dunn, *Technology-Facilitated Gender-Based Violence: An Overview,* Centre for International Governance Innovation: Supporting a Safer Internet Paper No. 1., 2021, p. 9.
[20] https://www.techtarget.com/whatis/definition/deepfake

fake is a form of image-based sexual abuse and AI-generated gender-based violence against women. As a matter of fact, in the majority of cases – studies show[21] – sexual deep fakes are forms of non-consensual pornography.

The VAW Directive also provides for the harmonisation of the elements of the crime of 'intentionally **inciting violence or hatred** directed against a group of persons or a member of such a group, defined by reference to gender, by publicly disseminating, by means of ICT, material containing such incitement is punishable as a criminal offence' (Article 8). In 2008, prior to the entry into force of the Lisbon treaty, the EU adopted a Framework Decision on combating certain forms and expressions of racism and xenophobia by means of criminal law.[22] The criminalisation of this behaviour is not new; the novelty in the VAW Directive concerns the grounds of hate, namely gender. Studies show that women face a backlash when exercising freedom of expression, including women politicians,[23] journalists and bloggers.[24] These attacks result in some women pulling out from public life or engaging in self-censorship. Hate speech is also directed against persons who manifest their opinions online and do not have a 'public' and 'popular' life. According to the European Institute for Gender Equality (EIGE): 'Women who have ideas that are considered radical, women challenging traditional gender roles, journalists and otherwise politically outspoken women face gendered threats and violence through Twitter and other social online forums. Being present in online spaces alone often means being present in a hostile, sexist environment.'[25] Countering hate speech based on sex/gender that takes place online or through digital technologies can enable women to fully participate in political, economic, and public life.[26]

The **discussion within the network** will be guided by three main points (MA.K.E.):

a) **MA**pping measures and approaches with regard to NCII abuse and cyber hate speech on the basis of gender, looking into gaps and emerging needs;

b) share **K**nowledge about the impact of cyber violence on women and girls;

c) **E**xchange existing good practices and effective outcomes.

Guiding questions for the introductory part:

General discussion with the audience before the presentation by the legal expert: How do you define NCII abuse? Could you mention its core elements (such as intent to hurt or the number of end-users, for example)?

Discussion around the tables:

- Has your country taken action on criminalisation of NCII abuse and cyber incitement to violence or hatred on the basis of gender after the adoption and the entry into force of the VAW Directive (multiple choice: political debate, civil society activism, media coverage, discussion of legislative proposals, other)?

[21] https://www.cigionline.org/articles/women-not-politicians-are-targeted-most-often-deepfake-videos/
https://theconversation.com/deepfake-porn-why-we-need-to-make-it-a-crime-to-create-it-not-just-share-it-227177

[22] Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, OJ L 328, 6.12.2008, pp. 55–58.

[23] European Institute for Gender Equality (EIGE), *Cyber violence against women and girls*, 2017, available at: https://eige.europa.eu/publications/cyber-violence-against-women-and-girls; Council of Europe Gender Equality Strategy, *Combating sexist hate speech*, 2016, available at: https://edoc.coe.int/en/gender-equality/6995-combating-sexist-hate-speech.html; Inter-Parlamentarian Union, *Sexism, harassment and violence against women parliamentarians*, 2016, available at: http://archive.ipu.org/pdf/publications/issuesbrief-e.pdf.

[24] FRA, *Violence, threats and pressures against journalists and other media actors in the European Union*, 2016, available at: https://fra.europa.eu/en/publication/2016/violence-threats-and-pressures-against-journalists-and-other-media-actors-european.

[25] EIGE (2017), *Cyber violence against women and girls,* cit., p. 9.

[26] See S. De Vido, L. Sosa, *Criminalisation*, cit.

- Is your country already (fully/partly/not at all: multiple choice) complying with the obligations stemming from the VAW Directive?
- Are there elements of the cybercrimes included in the VAW Directive that your Member State has identified as difficult to implement?

Panel 1 – Preventing NCII abuse

Several countries, as a report has shown, have decided in recent years to combat non-consensual dissemination of intimate/private/sexual images through specific criminal law provisions.[27] That said, criminalisation should not be the only action to counter the non-consensual dissemination of intimate/private/sexual images. Preventive measures, ranging from the training of professionals to the raising of awareness of the serious consequences of the behaviour at the societal level, along with protective measures for the victims/survivors should be considered.

Prevention is indeed a key part of the action to counter gender-based NCII creation and sharing. In the VAW Directive, several provisions refer to this aspect, which is also one of the pillars of the Istanbul Convention. Under Article 34 (8) VAW Directive, 'preventive measures shall specifically address the cybercrimes referred to in Articles 5 to 8. In particular, Member States shall ensure that such preventive measures include the development of **digital literacy skills,** including critical engagement with the digital world and critical thinking to enable users to identify and address cases of cyber violence, to seek support and to prevent its perpetration.'

In a community, in a group of people (family, friends, neighbours, colleagues), the identification of digital violence represents a tool for preventing NCII abuse. Education should also be aimed at explaining how to react as a bystander, fully respecting the victim but also without turning a blind eye to NCII creation and sharing. Furthermore, Member States shall 'foster multidisciplinary and stakeholder cooperation, including among relevant intermediary service providers and competent authorities, to develop and implement measures to address the cybercrimes referred to in Articles 5 to 8.' Article 35, despite focusing in particular on rape, stresses the role of consent in relationships. Consent is crucial in the prevention of NCII abuse because it is the absence of consent that characterises both the offense of creating the material and of sharing it (in the case of sharing, it is not relevant whether the person originally agreed or not to take the image or the video). The provision on education on consent is therefore relevant also for the prevention of NCII abuse. Concerning training, the Directive specifies that, having regard to the respect for freedom and pluralism of the media, Member State are obliged to 'encourage and support the setting up of media training activities by organisations of media professionals, media self-regulatory bodies and industry representatives or other relevant independent organisations to combat stereotypical portrayals of women and men, sexist images of women, and victim-blaming in the media, aiming to reduce the risk of violence against women or domestic violence' (Article 36(8)).

Even though the focus of the network is prevention, it should be noted that protection measures envisaged by the VAW Directive cover all forms of violence, hence including violence in the digital world. It means that, for example, given the obligation for States to establish state-wide telephone helplines, these services must be capable of providing information and advice to victims also with regard to NCII abuse. It also means that police forces must be capable of detecting gender-based NCII abuse and provide appropriate information and, if it is the case, referral to the units that specialise in computer crimes.

[27] S. De Vido, L. Sosa, *Criminalisation*, cit.

Practices and initiatives are important in the field and the purpose of this panel is to know more about domestic ones. For example, **StopNCII.org** is a free tool designed to support victims of Non-Consensual Intimate Image (NCII) abuse.[28] The tool works by generating a hash from your intimate image(s)/video(s). Image hashing is the process of using an algorithm to assign a unique hash value to an image. Duplicate copies of the image all have the exact same hash value. For this reason, it is sometimes referred to as a 'digital fingerprint'. In the UK, the **Revenge Porn Helpline** was established in 2015: it is a service supporting adults who are experiencing intimate image abuse.[29] An ongoing CERV project, called **SURF and SOUND** – Support, Unite, Respond, Fight to Stop Online violence 2.0, based in Croatia, improves already formed mechanisms of prevention and combating online violence like online platform NEON – No to Online Violence (information, advice and tools for self-protection and reporting). Awareness-raising activities will go further to inform the general population about the less recognized forms of online violence against women and to promote reporting on the local level and in smaller towns where victims are more often faced with shaming and blaming.[30]

Invited speaker: Sophie Mortimer, who manages the Revenge Porn Helpline and day-to-day aspects of StopNCII.org.

Discussion around the tables:

- How widespread is the phenomenon in your country? Are specific data available, such as surveys or administrative data? In the case of administrative data, are behaviours falling under NCII abuse coded as a standalone crime or together with others?
- Why is it difficult to get data with regard to NCII abuse?
- Are there protection measures envisaged in the case of NCII abuse? Are forms of NCII abuse considered in the risk assessment, for example? Are shelters accessible to victims of NCII abuse as well?
- Can you share practices or ideas on how to activate bystanders in preventing NCII abuse?

Panel 2 – Panel on communication

Participants will be asked before the meeting to suggest campaigns /actions/videos that promote digital literacy, online respect, online consent, the use of respectful language, etc.

A selection of videos will be projected (and translation provided whether necessary) and commented on by the participants. With the support of the videos, the discussion will specifically focus on how to avoid victim blaming in communication and how effectively to raise awareness of the potential risks of NCII abuse and hate speech.

DAY 2

Panel 3 – Panel on cyber hate speech on the basis of gender

Several countries, as a report has shown, have explicitly recognised sex or gender as a ground for hate speech, while an increasing number of countries include sexual orientation and/or gender identity and/or sex reassignment among the prohibited grounds.[31] In some cases, domestic laws have explicitly incorporated

[28] https://stopncii.org/?lang=en-gb
[29] https://revengepornhelpline.org.uk/
[30] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/43251589/101097052/CERV?order=DESC&pageNumber=1&pageSize=50&sortBy=title&keywords=%20cyber%20gender-based%20violence&isExactMatch=true&frameworkProgramme=43251589
[31] S. De Vido, L. Sosa, *Criminalisation*, cit.

gender in the enumeration of the grounds included in the definition of the offence; in other cases, laws incorporated sex/gender under the broader notion of 'other group' or similar, through case law or other policy documents. That said, criminalisation should not be the only action to counter incitement to hatred or violence. As it was said above with regard to NCII, preventive measures, ranging from the training of professionals to the raising of awareness of the serious consequences of the behaviour at societal level, along with protective measures for the victims/survivors should be considered.

Prevention is indeed a key part of the action to counter gender-based cyber hate speech. In the VAW Directive, several provisions refer to this aspect, which is also one of the pillars of the Istanbul Convention. Under Article 34 (8) VAW Directive, 'preventive measures shall specifically address the cybercrimes referred to in Articles 5 to 8. In particular, Member States shall ensure that such preventive measures include the development of **digital literacy skills,** including critical engagement with the digital world and critical thinking to enable users to identify and address cases of cyber violence, to seek support and to prevent its perpetration.' In a community, in a group of people (family, friends, neighbours, colleagues), the identification of digital violence represents a tool for preventing hate speech. Education should also be aimed at explaining how to react as a bystander, fully respecting the victim but also without turning a blind eye to hate speech. Furthermore, 'Member States shall foster multidisciplinary and stakeholder cooperation, including among relevant intermediary service providers and competent authorities, to develop and implement measures to address the cybercrimes referred to in Articles 5 to 8.' Concerning training, the Directive specifies that, having regard to the respect for freedom and pluralism of the media, Member States are obliged to 'encourage and support the setting up of media training activities by organisations of media professionals, media self-regulatory bodies and industry representatives or other relevant independent organisations to combat stereotypical portrayals of women and men, sexist images of women, and victim-blaming in the media, aiming to reduce the risk of violence against women or domestic violence (Article 36(8)).

Even though the focus of the network is prevention, it should be noted that protection measures envisaged by the VAW Directive cover all forms of violence, hence including violence in the digital world. It means that, for example, given the obligation for States to establish state-wide telephone helplines, these services must be capable of providing information and advice to victims also with regard to cyber hate speech. It also means that police forces must be capable of detecting gender-based cyber hate speech and provide appropriate information and, if it is the case, referral to the units that specialise in computer crimes.

Practices and initiatives are important in the field and the purpose of this panel is to know more about domestic ones. For example, in Italy, the ***Rete nazionale*** *per il contrasto ai discorsi e ai fenomeni d'odio* (National network to counter hate speech and hate behaviours) aims at mapping, preventing and combating hate speech and hate phenomena, which are increasingly pervasive and to which the *Rete Nazionale* wants to give a strong and effective response. The Italian network prepares newsletters with events and short papers, reacts to episodes of hate that occur in Italy through public statements, and engages in a strong activity of advocacy and education in schools.[32]
A **CERV project**, that has recently ended, is Fighting hAte Speech Through a Legal, ICT and Sociolinguistic approach. Among the outputs, of interest is the design and development of the **FAST LISA** dashboard, a specific tool designed on a state-of-the-art analysis covering legal, linguistic and sociological aspects of hate speech online. The dashboard uses big data from Facebook, Instagram, TikTok and others social networks to draw a sentiment analysis and artificial intelligence engine in order to classify the contents and produce

[32] https://www.retecontrolodio.org/advocacy/

visualization on the community maps.[33] Another CERV project is **CHASE**, which seeks to establish and put into practice in Cyprus, Italy, Greece and France, a comprehensive mechanism for online media to effectively detect and respond to cases of online gender-based hate speech.[34]

Invited speaker: Federico Faloppa, University of Reading, UK, coordinator of the Italian *Rete nazionale per il contrasto ai discorsi e ai fenomeni d'odio* (National network to counter hate speech and hate behaviours).

Guiding questions:
Discussion around the tables:

- How widespread is the phenomenon in your country? Are specific data available, such as surveys and administrative data? In the case of administrative data, is hate speech on the basis of gender coded as a standalone crime or together with others?
- Why is it difficult to get data with regard to hate speech on the basis of gender?
- Which measures are in place in your country (if any) to prevent cyber hate speech on the basis of gender?
- In terms of budget, how much money (% of the total) has been allocated to hate speech on the basis of gender compared to other grounds and why?

Panel 4 - Engaging online platforms and media – is it possible?

In FRA's opinion, expressed in a recent report of 2023:

> Online platforms should have specific regard to protected characteristics of users in the context of their terms and conditions, content moderation practices and monitoring policies, including addressing sexist online hate. Performance indicators should be in place to record the volume of misogyny online and the effectiveness of content moderation, looking at developments over time.[35]

As said above, the VAW Directive specifies that, having regard to the respect for freedom and pluralism of the media, Member States are obliged to 'encourage and support the setting up of media training activities by organisations of media professionals, media self-regulatory bodies and industry representatives or other relevant independent organisations to combat stereotypical portrayals of women and men, sexist images of women, and victim-blaming in the media, aiming to reduce the risk of violence against women or domestic violence' (Article 36(8)). The engagement of media not only to reduce the risk of violence against women and domestic violence but also to go back at the root causes of it, namely stereotypes, is evident in the newly-adopted Directive.

A relevant provision is Article 23 VAW Directive: **Measures to remove certain online material.** The provision is without prejudice to Regulation No. 2022/2065 and requires Member States to ensure that online publicly accessible material that refers to one of the offences in the Directive (non-consensual sharing of intimate or manipulated images, cyber harassment and cyber incitement to violence or hatred) are promptly removed or the access is disabled. There is a series of guarantees for the application of this article. Measures must include the possibility for the competent authorities to issue binding legal orders to hosting service providers to remove or to disable access to such material, which must respect, as a minimum, the conditions set out in Article 9(2) of Regulation (EU) 2022/2065. Where removal is not feasible, the provision

[33] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/43251589/101049342/CERV?order=DESC&pageNumber=1&sortBy=title&keywords=hate%20speech&isExactMatch=true&frameworkProgramme=43251589
[34] https://cesie.org/en/project/chase/
[35] FRA, *Online Content Moderation*, 2023, p. 10, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2023-online-content-moderation_en.pdf

requires the competent authorities to address orders to disable access to the material concerned to relevant intermediary service providers other than hosting service providers that have the technical and operational ability to take action regarding the material concerned. Procedures for the adoption of the order must be transparent and subject to adequate safeguards (necessity and proportionality). Freedom of expression and freedom of the press must be guaranteed.

The European Union adopted in 2016 a **Code of conduct** on countering illegal hate speech online, which addresses the need for online intermediaries to take action against hate speech posted by users on their services. The Code of conduct guides ICT companies in taking action against 'illegal hate speech' – according to relevant national laws transposing Council Framework Decision 2008/913/JHA - and to facilitate the elimination of flagged harmful comments from their platforms.[36] The European Commission has highlighted the complementarity of this instrument with the effective enforcement of existing legislation. It should also be noted that, as announced in the 2020-2025 Gender Equality Strategy, the Commission will facilitate a framework for cooperation between internet platforms to tackle online violence against women, in the form of a Code of Conduct.

Invited speaker: Catherine Van de Heyning, University of Antwerp catherine.vandeheyning@uantwerpen.be

Guiding questions:

Discussion around the tables:

- How can we prevent gender-based cyber hate speech and NCII abuse through the engagement of platforms and media? E.g.: national cooperation frameworks with internet platforms and/or national obligations or national codes of conduct for them on these issues
- There is a specific article of the VAW Directive on the removal of online material that amounts to one of the crimes included in the Directive. How effective is / can be /will be in your country? Would this give additional power to Member State or Equality Bodies or designated flaggers in removing content, in addition to the powers granted by the DSA?
- Do you think a code of conduct specifically focused on cyber violence would be useful? What should this Code of Conduct entail?

Conclusions

In a final session, the main points of the discussion will be summed up, and further suggestions collected from the participants on the role of the EU in the implementation of the VAW Directive and of the Istanbul Convention within the limits of EU competences.

[36] Code of conduct on countering illegal hate speech online, 30 June 2016, available at: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en.